Symmetry and Randomness in Quantum Information Theory: Several Applications

by

Wei Xie

A dissertation submitted for the degree of

Doctor of Philosophy

Centre for Quantum Software and Information
Faculty of Engineering and Information Technology
University of Technology Sydney, Australia

Certificate of Original Authorship

I, Wei Xie, declare that this thesis is submitted in fulfilment of the requirements for the award of PhD in the School of Computer Science at the University of Technology Sydney. This thesis is wholly my own work unless otherwise reference of acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis. This document has not been submitted for qualifications at any other academic institution. This research is supported by the Australian Government Research Training Program.

Production Note:
Signature removed
prior to publication.

Abstract

This thesis studies four topics in quantum information theory using tools from representation theory and (high-dimensional) probability theory.

First, we study the nonadditivity of minimum output von Neumann and Rényi entropy of quantum channels. A sketch of the proof by Aubrun, Szarek and Werner for nonadditivity of minimum output entropy is presented, and a slight simplification is given. We show that asymptotically the minimum output entropy of the random channel $\mathcal{E} \otimes \mathcal{E} \otimes \mathcal{E}^*$ is achieved not by a tripartite genuinely entangled state, but by a tensor product of two states. We also study another model of random channel, and our estimation of the minimum output Rényi entropies fails to show the usefulness of genuine multipartite entanglement for the multiple nonadditivity.

Second, we study the generic entanglement in the random near-invariant tensors under the action of $\mathfrak{su}(2)$, and random symmetric invariant tensors under the action of $\mathfrak{su}(d)$ for any d, serving as an extension of the random invariant tensors under $\mathfrak{su}(2)$. We show that both the random tensors are asymptotically close to a maximally entangled state with respect to any bipartite cut.

Third, we study efficient quantum certification for states and unitaries. We present an algorithm that uses $O(\varepsilon^{-4} \ln |\mathcal{P}|)$ copies of an unknown state to distinguish whether the unknown state is contained in or ε-far from a finite set $\mathcal{P}$ of known states with respect to the trace distance. This algorithm is more sample-efficient in some settings. The previous study showed that one can distinguish whether an unknown unitary U is equal to or ε-far from a known or unknown unitary V in fixed dimension with $O(\varepsilon^{-2})$ uses of the unitary, in which an ancilla system should be used. We give an algorithm that distinguishes the two cases with $O(\varepsilon^{-1})$ uses of the unitary, without using ancilla system or using ancilla system of much smaller dimension.

Finally, we study the parallel repetition of extended nonlocal game motivated by its connection with multipartite steering and entanglement de-

tection. We show that the probability of winning an n-fold parallel repetition of commuting nonsignaling extended nonlocal game G decreases exponentially in n, provided that the game value of G is strictly less than 1, following the approach used by Lancien and Winter based on de Finetti reduction.

Contents

Notation

Here is a list of some notation frequently used in this thesis, along with its description unless otherwise noted.

ln	Natural logarithm
log	Binary logarithm
$\mathbb{N}$	The set of all nonnegative integers
$\mathbb{Z}$	The set of all integers
$\mathbb{R}$	The set of all real numbers
$\mathbb{C}$	The set of all complex numbers
$[m]$	The set $\{1, 2, \ldots, m\}$
$\Pr(E)$	Probability of event E
$\mathbb{E}X$	Expectation of random variable X
$\mathrm{Var}X$	Variance of random variable X
M^T	Transpose of matrix M
M^*	Complex conjugate of matrix M
$M^\dagger$	Transpose conjugate of matrix M
$M \geq N$	$M - N$ is semidefinite positive for Hermitian M, N
$\|M\|_p$	Schatten p-norm of matrix M
$\langle u, v \rangle$	Equal to $\sum_i u_i^* v_i$ for vectors u, v
$\langle M, N \rangle$	Equal to $\mathrm{tr}(M^\dagger N)$ for matrices M, N
$\mathcal{H}, \mathcal{K}$	Typical (finite-dimensional) Hilbert spaces
$\mathcal{L}(\mathcal{H}, \mathcal{K})$	The set of all linear operators from $\mathcal{H}$ to $\mathcal{K}$
$\mathcal{L}(\mathcal{H})$	$\mathcal{L}(\mathcal{H}, \mathcal{H})$
$f \lesssim g$	For positive functions f, g of n, $f(n) \leq cg(n)$ holds for some positive constant c and any sufficiently large n, also written as $g \gtrsim f$, or $f = O(g)$, or $g = \Omega(f)$
$f \simeq g$	Both $f \lesssim g$ and $f \gtrsim g$ hold, also written as $f = \Theta(g)$
$f \sim g$	$f(n)/g(n) \to 1$ as $n \to \infty$

$\mathrm{U}(d)$	Unitary group of degree d
$\mathrm{SU}(d)$	Special unitary group of degree d
$\mathrm{SL}(d)$	Special linear group of degree d over $\mathbb{C}$
$\mathrm{GL}(d)$	General linear group of degree d over $\mathbb{C}$
$\mathfrak{su}(d)$	Lie algebra of $\mathrm{SU}(d)$
$\mathfrak{sl}(d)$	Lie algebra of $\mathrm{SL}(d)$ over $\mathbb{C}$
$\mathrm{Par}(n)$	The set of all partitions of n
$\lambda \vdash n$	$\lambda \in \mathrm{Par}(n)$
$\mathrm{Par}(n, d)$	The set of all partitions of n with length at most d
$\mathrm{Type}(n, d)$	The set of all types of strings in $\{1, 2, \ldots, d\}^n$
R	The function that maps a group or an algebra to the set of its representation matrices
S_n	Symmetric group of degree n
W_π	The operator that permutates n tensor factors according to $\pi \in S_n$
W	Typical name for the swap operator
V_λ^L	The irrep of $\mathrm{GL}(d)$ of highest weight λ, sometimes written as V_λ or $\mathcal{H}_\lambda$
V_λ^S	The irrep of S_n labeled by partition λ, sometimes written as $\mathcal{K}_\lambda$
$\vee^n \mathbb{C}^d$	The symmetric subspace of $(\mathbb{C}^d)^{\otimes n}$
$\wedge^n \mathbb{C}^d$	The antisymmetric subspace of $(\mathbb{C}^d)^{\otimes n}$
χ	Character of a representation, or Holevo information, or Holevo capacity
$\mathcal{S}^{d-1}$	Unit sphere in Euclidean space $\mathbb{R}^d$
$\mathcal{S}(\mathcal{H})$	Unit sphere in Hilbert space $\mathcal{H}$
$\mathcal{D}(\mathcal{H})$	The set of all density operators on $\mathcal{H}$
ρ, σ	Typical density operators
ψ, φ	$\psi = \lvert\psi\rangle\langle\psi\rvert$, $\varphi = \lvert\varphi\rangle\langle\varphi\rvert$ (applied for all pure states)
ϕ, ω	Typical maximally entangled state and maximally mixed state respectively
$H_p(\cdot)$	(Quantum or classical) p-Rényi entropy
$H(\cdot)$	Shannon entropy, or von Neumann entropy
$\mathrm{D}(\rho, \sigma)$	Trace distance between two quantum states ρ, σ
$\mathrm{F}(\rho, \sigma)$	Fidelity between two quantum states ρ, σ